Melanie Miller

Partner
Technology Assurance
Tel: +27 82 717 0195
Email: melanie.miller@kpmg.co.za

Ashaylan Moodley

Associate Director
Technology Assurance
Tel: +27 82 719 2738
Email: ashaylan.moodley@kpmg.co.za

Gabriella Pesquito

Senior Analyst
Technology Assurance
Tel: +27 63 645 4601
Email: gabriella.pesquito@kpmg.co.za

Navigating the technology impact of Joint Standard 1 of 2023 on the insurance industry

The recently released regulation issued jointly by the Prudential Authority (PA) and the Financial Sector Conduct Authority (FSCA), Joint Standard 1 of 2023[1] ('Joint Standard 1' or 'the standard'), focusses on IT governance and risk management. The standard is expected to have a significant impact on the insurance industry through increased governance requirements that are to be complied with ultimately by the board of directors (or equivalent governing body).

IT risk management and governance has always been high on the agenda for organisations and many of the principles outlined in the standard are not new considerations. The standard, however, now mandates the following requirements which may not always have been high priority:

- enhanced documentation of risks and controls, noting responsible stakeholders;
- being able to report on IT governance to the regulator upon request; and
- obtaining assurance on IT-related governance structures that may have not been subject to assurance previously.

[1] https://www.resbank.co.za/en/home/publications/publication-detail-pages/prudential-authority/pa-public-awareness/Communication/2023/Joint Communication-4-of-2023-Publication-of-the-Joint-Standard-IT-Gov-and-Risk

Tabled below are the key requirements of Joint Standard 1, what this means for insurers and principle questions that the board will need to address:

Requirement	What this means for insurers	Questions for the board
1. Enhanced IT governance Ultimately, the board of directors is now directly responsible for ensuring continuous compliance with Joint Standard 1 of 2023. The standard requires insurers to develop an IT strategy which aligns to the overall business strategy. In addition, comprehensive IT governance frameworks should align with the organisation's overall corporate governance framework, with the goal of deriving improved value from investment in technology.	To ensure that the overall governance frameworks are aligned to IT-specific governance frameworks and that organisational IT policies and standards are updated to reflect this alignment. Management may face challenges when incorporating IT risks into the overall business risk assessment and applicable governance mechanisms with a single point of accountability.	• Have we reviewed the IT strategy against the overall business strategy to ensure alignment and have we decided on how often this should be reviewed? • Have we ensured that the alignment of general business strategy and governance updates occur alongside the related IT requirements as part of the annual governance cycle? • Have we recently reviewed our governance frameworks against IT frameworks and ensured alignment? • Are our business and IT stakeholders convening regularly to ensure alignment and adapting governance frameworks as appropriate? • How often should we, as the board of directors, be assessing compliance with Joint Standard 1 to ensure that compliance is continuously being met, including obtaining periodic representation from key business stakeholders to support this requirement? • What mechanisms do we need to put into place to ensure that any instances of non-compliance with Joint Standard 1 are reported and remediated in a timely manner?
2. Focus on risk management The standard requires financial institutions (including insurers) to develop an IT risk management framework and regularly conduct risk assessments which aim to identify potential threats and mitigate the risk of these threats materialising. The standard aims to encourage insurers to adopt a proactive approach in building defences against potential disruptions.	To ensure that an effective risk management framework is managed and linked to risk assessments conducted by management. Management may face challenges in performing risk assessments and implementing responses to these risks in a timely manner. Further challenges include ensuring that controls implemented effectively mitigate the risk to operate consistently.	• Does our risk register account for all IT risks noted in the standard? • Do we have an IT risk management framework that notes the frequency of risk assessments, who is responsible for conducting the risk assessments and how these risks will be managed, reported and documented?
3. Outsourcing and third-party management Insurers are urged to identify, assess and manage third-party agreements and associated risks relating to technology providers*. **This is covered in a separate Joint Standard – refer to the link in footnote 2[2].*	To ensure that IT risks relating to third-parties are considered and managed with appropriate mitigations implemented. Management may face challenges in adequately identifying relevant third-party risks by not fully understanding third-party operational environments and may also face challenges in confirming that third-party risks are appropriately addressed, either by the third-party or by the insurer's internal control processes.	• Have we identified all third-parties that our organisation engages with and is exposed to? • Have we performed risk assessments over these third-parties and ensured that we have identified mitigations prioritised to key third-parties? • Have we built risk assessment measures into our contracts with third-parties, where possible? • Have we obtained assurance (e.g. SOC reports) from our third-parties to ensure that the relevant technology risks have been effectively managed? • Have we identified Complementary User Entity Controls specified in the assurance reports from third-parties and have these been effectively implemented into our organisation?

[2] https://www.resbank.co.za/content/dam/sarb/publications/prudential-authority/pa-public-awareness/covid-19-response/2024/joint-comms-1-of-2024/Joint%20Standard%201%20of%202024%20Outsourcing%20by%20Insurers.pdf

Requirement	What this means for insurers	Questions for the board
4. Reporting to the regulatory authority Insurance institutions are required to notify the regulatory authority in the event of system failures, malfunction, delay or any disruptive events.	To ensure that any disruptive events are reported to the regulator and that the risk of non-compliance in the event of failure to report, is managed effectively. Management may face difficulty in ensuring that an effective process is in place to identify relevant risk events across the organisation and that they are reported to relevant stakeholders in a timely manner.	• Have we defined the disruptive events that are to be reported to the regulator to ensure compliance? • Is there an established process, including internal stakeholder engagement, to enable reporting in a timely manner? • Do we know which individual or function is tasked with regulatory reporting per our defined definitions of disruptive events?
5. Protection of data In developing an IT strategy, insurance companies are required to incorporate processes that maintain the confidentiality and integrity of data, such as: • identifying and managing the risk associated with financial products; • ensuring backup systems and procedures and business continuity plans are in place; • access control mechanisms; and • maintaining services that are managed by third-parties.	The everchanging nature of technology has resulted in record numbers of privacy violations and cybersecurity incidents. The standard places emphasis on the importance of client information and the safeguarding thereof. The standard urges insurers to make use of measures to protect client information such as: • access control mechanisms; • continuous compliance with regulatory data protection standards; and • encryption of data. IT processes that can be implemented to ensure business continuity include, but are not limited to: • vulnerability assessments; • penetration testing; • incident response plans which delve into root cause analysis and lessons learnt; and • consideration of technologies that provide insight into emerging threats.	• Do we have effective response mechanisms in place relating to data protection, cybersecurity and resilience and business continuity risks? • How often are these response mechanisms reviewed and reassessed to consider new or evolving risk exposures? • Do these responses include the formalisation of specific policies, procedures and effective reporting, as well as clearly defined responsibilities and functions that own the technology risks?

Challenges faced by organisations

1. Resource intensive

For small to medium organisations, co-ordinating and implementing comprehensive IT governance and risk management frameworks, structures and policies are costly and skills intensive. A balance between compliance and operational cost management is imperative. Small to medium insurers have implemented different strategies to overcome the cost and resource intensiveness of co-ordinating and implementing comprehensive IT governance frameworks, as noted below:

- Cloud services provide insurers with the opportunity to leverage off the reduced need for on-premise intrinsic infrastructure which lowers the cost of the management of IT.
- Insurers have moved towards outsourcing IT functions or collaborating with organisations that specialise in the management of IT. Although this introduces different risks to insurers, this mechanism allows insurers to access appropriate expertise and information technology infrastructure at a lower cost than that of in-house development.
- By implementing AI and automation, insurers can leverage off streamlining business and IT processes, remove the element of manual intervention, reduce the risk of error and increase the efficiency of reporting. This not only increases precision but contributes towards costs reduction.
- Investing time and effort into the training and development of employees will ensure that staff are well-versed in terms of IT governance procedures, practices and maintenance. Management will benefit from redefining the roles of IT staff to include performance of control activities with a focus on governance, highlighting that IT roles are no longer limited to execution activities but also includes evidencing sound governance activities as part of their execution.

2. Adaptation period

Insurance institutions are known for operating complex and intricate systems. The process of organisations adapting to the new standard may involve significant changes to existing IT infrastructure, frameworks, policies and structures. Insurance institutions face the possibility of experiencing disruption, as a result of adapting to requirements, and this could in turn impact day-to-day operations due to vulnerabilities.

The implementation of Joint Standard 1 can be sub-categorised into three phases: current, transition and future. The current phase speaks to identifying where insurers are in terms of Joint Standard 1 maturity. The future state is the desired place the insurer would like to be, i.e. in ensuring compliance with Joint Standard 1. The transition phase is thus the most critical phase of the implementation cycle as insurers need to clearly define and identify the temporary measures that need to be implemented in moving from the current state to the future state.

As an example, large volumes of data are maintained by insurance companies. As a starting point in the current phase, it is imperative for the organisation to identify critical data to the organisation and the risks that will materialise if that data is compromised due to a lack of IT information security governance. In order to get to the desired future state of being secure, there are certain measures that should be put in place during the transition phase. Examples of these measures include the encryption of customer data at rest and in transit which can be achieved using encryption algorithms. In conjunction, the use of access controls in implementing least privilege access would result in granting users access only to the data they need to perform job duties.

3. Evolution of threats

While the standards address current IT concerns, the fast-evolving nature of cyber threats raises questions about the long-term relevance of the prescribed measures. Insurance institutions must remain agile and continually update their defences to stay ahead of emerging risks, requiring a sustained commitment to ongoing adaptation and improvement.

The National Institute of Standards and Technology (NIST) framework is widely regarded as a benchmark for managing and mitigating cyber risks. It provides a structured approach to identifying, protecting, detecting, responding to and recovering from cyber incidents. Insurers often adopt this framework to tailor their defences based on specific risk profiles. The regular performance of risk assessments provides insurers with a basis to remain informed on potential threats and vulnerabilities that exist within the IT environment. This is not limited to the insurer's system landscape but also the risk of third-party vendors and external stakeholders. Insurers can also benefit from joining information-sharing organisations such as the Financial Services Information Sharing and Analysis Center (FS-ISAC), which facilitates the exchange of threat intelligence and emerging cyber risks within the industry. This helps insurers maintain real-time awareness of cyber threats.

Insurers are increasingly shifting towards a Zero Trust Architecture, which mandates continuous verification of access requests, regardless of whether they originate inside or outside the network. This approach limits the likelihood of successful breaches by restricting access based on user identity and device security.

Additionally, insurers often conduct simulated cyber-attacks, such as phishing tests, to assess employee preparedness and improve their ability to identify and respond to threats. Insurers are encouraged to continuously perform vulnerability scans and penetration tests to uncover weaknesses within systems and mitigate these weaknesses before they can be exploited by malicious actors. The maintenance of a well-documented and tested incident response plan, that includes roles and responsibilities, communication strategies, and post-incident analysis to ensure swift recovery, is imperative.

Insurers are also encouraged to maintain awareness of regulatory guidelines, such as the General Data Protection Regulation, Protection of Personal Information Act and Joint Standards, which outline security requirements. Collaboration with regulators can also enhance preparedness for emerging threats.

Lessons learnt and insights gained from previous technology-related regulatory implementations

1. Management controls, while possibly adequate, may not always be appropriately evidenced

Our observations indicate that while management may have designed and implemented adequate controls as a response to the identified risk, there is a lack of audit trail to evidence that these controls are consistently performed by management, making it difficult to confirm that controls are operating effectively.

2. Control reporting

To collate the required information and align with relevant stakeholders within an organisation is not always straightforward. As controls serve multiple purposes to address operational, financial reporting or regulatory risks, controls can be at different levels of maturity for each business area and therefore may not be well documented and tracked for effectiveness. Reporting on control effectiveness, to cover the requirements of the standard, may prove to be a challenge when controls are maintained across divisions without a uniform reporting structure. Legacy reporting structures will need to be adjusted to allow for reporting at an organisational level in a timely manner.

3. Assurance fatigue

With the technology landscape always receiving heightened levels of attention due to the associated risk, it is of no surprise that multiple streams of assurance may be required by various stakeholders to appropriately manage this risk. This can range from internal assurance (internal audit), external assurance (mandatory external audit or ISAE 3402/SOC engagements for service providers), and focused regulatory audits. This places a resource capacity burden on IT staff and management to provide input to various assurance providers, whilst also maintaining a focus on executing day-to-day tasks required to effectively maintain the IT landscape and operations.

The benefits of complying with Joint Standard 1

The benefits extend far beyond just being compliant. Joint Standard 1 provides insurers with an opportunity to establish a culture of risk awareness through regular conversation on risk appetite and risk tolerance. More importantly, it provides insurers with the opportunity to align IT risk management efforts with that of the rest of the business. For insurers to fortify their strategy, integration with cybersecurity and third-party risk assessment is key, to ultimately understand how the strategy of the organisation is impacted by risks related to IT.

Insurers will realise the benefits of Joint Standard 1 by harnessing lessons learnt from the outcomes of incidents within their own environment, understanding the root cause of these incidents and the remediation required over risks and controls.

Conclusion

Joint Standard 1 of 2023 reshapes the landscape of IT governance for South African insurers. The overall impact on insurers will include short-term disruption to day-to-day activities as management embeds control and reporting mechanisms to complement business as usual activities. The long-term benefit will be enhanced insights into the organisation’s technology landscape and mitigation of IT related incidents, which ultimately promotes an IT resilient organisation. The integration of IT risk and governance activities as part of an overall risk strategy allows the board to have a holistic view of risks and controls.